

**UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA**

Melissa Thomas, on behalf of herself  
individually and on behalf of all others  
similarly situated,

Plaintiff,

v.

Pawn America Minnesota, LLC, Payday  
America, Inc., and PAL Card Minnesota,  
LLC.,

Defendants.

Case No. 0:21-cv-2554

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff Melissa Thomas (“Plaintiff”), on behalf of herself and all others similarly situated (the “Class Members”), brings this Class Action Complaint against Defendants Pawn America Minnesota, LLC; Payday America, Inc.; and PAL Card Minnesota, LLC (collectively “Pawn America” or “Defendants”). The allegations in this Complaint are based on the personal knowledge of Plaintiff or upon information and belief and investigation of counsel.

**NATURE OF CASE**

1. Defendants are, on information and belief, a commonly owned and operated alternative financing business with operations principally focused in Minnesota and Wisconsin.

2. According to its website, Defendant Pawn America Minnesota, LLC operates 17 pawn shops in Minnesota and Wisconsin, having been founded approximately thirty years ago.<sup>1</sup>

3. Defendant Payday America, Inc. “has been providing guests with short-term banking options for more than a decade. [It] currently operate[s] 12 stores throughout Minnesota.”<sup>2</sup>

4. Defendant PAL Card Minnesota, LLC operates under the trade name of CashPass marketing, distributing, and supporting prepaid payment cards.

5. All three of these entities are operated out of the same location in Burnsville, Minnesota, with the same manager or chief executive and, on information and belief, have integrated the computer systems of these three entities into one network.

6. Each of these entities collects personally identifying information (“PII”) on its customers, including account numbers, driver’s license information, social security numbers, names, addresses, phone number, email address, driver’s license number, social security number, passport number or other identification numbers.

7. On October 3, 2021, each Defendant discovered that a data breach (the “Data Breach”) had occurred approximately five days earlier.<sup>3</sup>

---

<sup>1</sup> <https://www.pawnamerica.com/about-pawn-america>

<sup>2</sup> <https://www.paydayamerica.com/about-us/> (last visited Nov. 23, 2021).

<sup>3</sup> Payday America, Inc. disclosure:

<https://apps.web.maine.gov/online/aeviewer/ME/40/50d22a46-3439-41ac-a535-8c1f7e071fde.shtml> (last visited Nov. 23, 2021); Pawn America Minnesota, LLC disclosure: <https://apps.web.maine.gov/online/aeviewer/ME/40/e7251389-a447-43f1-b677-a6e75d5050ba.shtml> (last visited Nov. 23, 2021); PAL Card Minnesota, LLC

8. Defendants have stated that:

On September 28th, 2021 we began experiencing outages and discovered that the company was the victim of a ransomware attack and some of our computer systems were compromised and encrypted. A forensic investigation determined that sometime on September 28th, 2021, a cybercriminal gained access to portions of the company's computer system and deployed various network reconnaissance and ransomware tools to gain access to portions of the system, and render them inaccessible to us. We have since restored our data from separate backup servers. The cybercriminal also informed us that they retained copies of much of the data and threatened to leak the information which could make it available to other cybercriminals.

9. According to Defendants' reports, as many as 500,000 (or more) customers may have had their personally identifiable information ("PII") obtained by unauthorized third parties. While Defendants were able to regain control of their system, the malicious third party retains Plaintiff's and Class Members' PII.

10. Plaintiff and Class Members are now faced with a present and imminent lifetime risk of identity theft. These risks are made all the more substantial because of the inclusion of Social Security numbers and other identifying information.

11. PII has great value to cyber criminals. As a direct cause of Defendants' Data Breach, its customers' PII is available and may be for sale on the dark web for criminals to access and abuse. Defendants' customers face a current and lifetime risk of identity theft.

12. Defendant PAL Card Minnesota, LLC acknowledges that "[i]t is our responsibility to protect the information shared with us."<sup>4</sup> Defendants, however, have failed this responsibility.

---

disclosure: <https://apps.web.maine.gov/online/aeviewer/ME/40/a52197b9-ae74-432d-9f9c-070ccc993c6f.shtml> (last visited Nov. 23, 2021).

<sup>4</sup> <https://www.cashpass.com/cybersecuity-incident-notice> (last visited Nov. 23, 2021).

13. The modern cyber-criminal can use the information stolen in cyber-attacks to assume a victim's identity when carrying out criminal acts such as:

- a. Using their credit history;
- b. Making financial transactions on their behalf, including opening credit accounts in their name;
- c. Impersonating them via mail and/or email;
- d. Stealing benefits that belong to them; and/or
- e. Committing illegal acts which, in turn, incriminate them.

14. Plaintiff and Class Members' PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect Plaintiff's and Class Members PII. Defendants not only failed to prevent the Data Breach, but after discovering the Data Breach, Defendants waited many weeks to report it to states' Attorney General, and to affected individuals such as Plaintiff and members of the Class.

15. As a result of Defendants' delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

16. Plaintiff brings this action on behalf of all persons whose PII was compromised because Defendants failed to:

- (i) adequately protect consumers' PII entrusted to it;
- (ii) warn its current and former customers, potential customers, and current and former employees of their inadequate information security practices; and

- (iii) effectively monitor their websites and platforms for security vulnerabilities and incidents.

Defendants' conduct amounts to negligence and violates federal and state statutes.

17. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include:

- (i) lost or diminished inherent value of PII;
- (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;
- (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time;
- (iv) the continued and increased risk to their PII, which, (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

### **PARTIES**

18. Plaintiff Melissa Thomas is a citizen of the city of Hudson, in St. Croix County, in the State of Wisconsin. Ms. Thomas received a Notice of the Data Breach from Defendants dated November 19, 2021, nearly eight weeks after the Data Breach. The Notice advised that the Data Breach had occurred following a "ransomware attack" where "a cybercriminal gained access to portions of the company's computer system and developed various network reconnaissance and ransomware tools to gain access to portions of the system." "The cybercriminal also informed [Defendants] that they retained copies

of much of the data and threatened to leak the information which would make it available to other cybercriminals.” This letter informed Ms. Thomas that her PII was involved.

19. Defendant Pawn America Minnesota LLC is a limited liability company formed under the laws of the State of Minnesota, with its principal place of business at 181 River Ridge Circle South in the City of Burnsville, County of Dakota, State of Minnesota.

20. Defendant Payday Minnesota, Inc. is a corporation formed under the laws of the State of Minnesota, with its principal place of business at 181 River Ridge Circle South in the City of Burnsville, County of Dakota, State of Minnesota.

21. Defendant PAL Card Minnesota, LLC is a limited liability company formed under the laws of the State of Minnesota, with its principal place of business at 181 River Ridge Circle South in the City of Burnsville, County of Dakota, State of Minnesota.

### **JURISDICTION AND VENUE**

22. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

23. This Court has personal jurisdiction over Defendants as Defendants’ principal places of business are located within this District.

24. Venue is proper in this Court under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District, Defendants reside within this judicial district, and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

### **FACTUAL ALLEGATIONS**

#### **Background**

25. In the ordinary course of doing business with Defendants, customers, like Plaintiff, and prospective customers are required to provide Defendants with sensitive PII such as:

- a. Full names;
- b. Social Security numbers;
- c. Driver's license numbers;
- d. Passport numbers;
- e. Government identification numbers;
- f. Dates of birth; and
- g. Financial account information;

26. Defendant Pawn America Minnesota LLC, provides a privacy policy on its website, speaking for the other Defendants as part of the "Rixmann Companies," wherein it states that "we take the protection of your personal information very seriously."<sup>5</sup>

---

<sup>5</sup> <https://www.pawnamerica.com/privacy-policy> (last visited Nov. 23, 2021).

27. Defendant PAL Card Minnesota, LLC provides for its customers a similar privacy policy.<sup>6</sup>

28. Defendant Payday America, Inc., in its privacy policy, informs its customers that it is “committed to the security and confidentiality of your non-public personal information. Our security practices include limiting access to this information to those employees and business associates with appropriate authority and for intended business purposes only.”<sup>7</sup>

29. Defendant Payday America Inc. promises that “To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.”<sup>8</sup>

### **The Data Breach**

30. On or about September 28, 2021, Defendants experienced issues with access its customers’ PII and other data due to as third party encrypting certain portions of Defendants’ networks.

31. A forensic investigation determined that this was due to a ransomware attack on Defendants’ internal network.<sup>9</sup>

---

<sup>6</sup> See privacy policy link at <https://www.cashpass.com/disclosures/> (last visited Nov. 23, 2021).

<sup>7</sup> See privacy policy link at <https://www.paydayamerica.com/about-us/> (last visited Nov. 23, 2021)

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*



32. In disclosures to the Maine Attorney General, Defendants all stated that the Breach was discovered on October 3, 2021.<sup>10</sup>

33. However, despite first learning of the Data Breach on or about October 3, 2021, Defendants did not take any “measures” to notify affected Class Members until at least October 25, 2021, with affected Class Members not being sent notice until November 19, 2021. It was at that time Plaintiff and members of the Class were told that “[t]he cybercriminal also informed us that they retained copies of much of the data and threatened to leak the information which could make it available to other cybercriminals.”

34. Additionally, though Plaintiff and Class members have an interest in ensuring that their information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures taken to ensure a breach does not occur again have not been shared with regulators or Class members.

35. While Defendants’ respective websites bear a link to a notice of the Data Breach dated October 25, 2021, a Class member, if any, who may have seen this notice, but who did not receive any notice of Data Breach from Defendants, would likely conclude that their data was not impacted in the Data Breach and, therefore, would not have known of the need to take action to protect themselves.

---

<sup>10</sup> *Supra*, n.3.

36. Defendants have not offered any identity theft monitoring services or assistance, other than the contact information for the Federal Trade Commission, and a link to the website of the Federal Trade Commission (“FTC”).<sup>11</sup>

### **Defendants Were Aware of the Data Breach Risks**

37. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

38. Plaintiff and Class Members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to employ reasonable care to keep such information confidential and secure from unauthorized access.

39. Defendants’ data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the banking/credit/financial services industry preceding the date of the breach.

40. Indeed, data breaches, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants’ industry, including Defendants.

---

<sup>11</sup> <https://www.identitytheft.gov/#/> (last visited Nov 23, 2021).

41. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.<sup>12</sup> Identity thieves use the stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.<sup>13</sup>

42. The PII of Plaintiff and Class Members was taken by cyber criminals for the very purpose of engaging in identity theft, or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

43. Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, driver's license numbers and/or state identification numbers, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result of a breach.

---

<sup>12</sup> See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), <https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf> (last visited Nov. 23, 2021).

<sup>13</sup> *Id.* The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 CFR § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” *Id.*

44. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

45. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

### **Defendants Failed to Comply with FTC Guidelines**

46. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

47. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

48. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

49. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

50. Defendants failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

51. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered;
- b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like

Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

- c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;
- d. Configure firewalls to block access to known malicious IP addresses;
- e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;
- f. Set anti-virus and anti-malware programs to conduct regular scans automatically;
- g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;
- h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;
- i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;
- j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;
- k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;
- l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;
- m. Execute operating system environments or specific programs in a virtualized environment; and

- n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

52. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

1. **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
2. **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).
3. **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
4. **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it.
5. **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

6. **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
7. **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.<sup>14</sup>

53. Defendants were at all times fully aware of their obligation to protect the PII of customers, prospective customers, and employees. Defendants were also aware of the significant repercussions that would result from their failure to do so.

#### **Defendants Failed to Comply with Industry Standards**

54. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

55. Defendant Payday America, Inc.'s privacy policy expresses a compliance with federal law required for "financial companies," as well as "limiting access to this information to those employees and business associates with appropriate authority and for

---

<sup>14</sup> <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Nov. 23, 2021).



intended business purposes only.” This policy refers to the remaining Defendants as “financial companies” as well, and states that federal law applies to the protection and sharing of information. The other Defendants’ privacy policies do not make such disclosures as “financial companies.”

56. Upon information and belief, Defendants failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendants’ industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

57. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach.

### **PII Holds Value to Cyber Criminals**

58. Businesses, such as Defendants, that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers may be tempting targets for hackers, but information such as dates of birth and Social Security numbers are

even more attractive to cyber criminals; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

59. The PII of individuals such as Plaintiff and Class Members remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>15</sup>

60. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration (“SSA”) stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>16</sup>

61. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant

---

<sup>15</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs> (last visited Nov. 23, 2021).

<sup>16</sup> *Identity Theft and Your Social Security Number*, <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Nov. 23, 2021).

paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Furthermore, as the Social Security Administration warns:

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. Sousing a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security Number, you should not be able to use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.<sup>17</sup>

63. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and Class Members stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and Class Members. Stolen personal data of Plaintiff and Class Members represents essentially one-stop shopping for identity thieves.

64. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII,

---

<sup>17</sup> *Id.*

understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

65. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office (“GAO”) Report to Congressional Requesters:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>18</sup>

66. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A “cyber black-market” exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiff and Class Members has a high value on both legitimate and black markets.

67. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver’s license or identification card in the victim’s name but with another’s picture, and/or using the victim’s information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

---

<sup>18</sup> See <https://www.gao.gov/assets/gao-07-737.pdf> (June 2007) at 29 (last visited Nov. 23, 2021).

68. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendants' former and current customers and employees whose Social Security numbers have been compromised now face a real, present, imminent, and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

69. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because those victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver's license number or government-issued identification number, name, and date of birth are durable.

70. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."<sup>19</sup>

71. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to

---

<sup>19</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Nov. 23, 2021).

police. An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

### **Plaintiff's and Class Members' Damages**

72. Defendants entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

73. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

74. Plaintiff and Class Members presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

75. Plaintiff and Class Members have been, and currently face substantial risk of being targeted now and in the future, subjected to phishing, data intrusion, and other illegality based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

76. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

77. Plaintiff and Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

78. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

79. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach

80. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

81. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

82. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

**Plaintiff Melissa Thomas's Experience**

83. Plaintiff Thomas has made purchases in person from one or more of the Defendants. Plaintiff Thomas has also returned a purchased item to one or more Defendants, which was re-purchased by providing Plaintiff Thomas a PAL Card populated with the amount of the re-purchase price, which she then deposited in her bank account.

84. In making these transactions, Plaintiff Thomas entrusted her PII and other confidential information to Defendants with the reasonable expectation and understanding that Defendants would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff Thomas would not have used Defendants' services had she known that Defendants would not take reasonable steps to safeguard her sensitive PII.

85. Plaintiff Thomas has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.



86. Plaintiff Thomas stores all documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the few online accounts that she has.

87. Plaintiff Thomas has suffered actual injury in the form of damages to, and diminution in, the value of her PII – a form of intangible property that Plaintiff Thomas entrusted to Defendants. This PII was compromised in, and has been diminished as a result of, the Data Breach.

88. Plaintiff Thomas has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

89. Plaintiff Thomas has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII resulting from the compromise of her PII, especially her Social Security number, in combination with her name, address, phone number, and email address, which PII is now in the hands of cyber criminals and other unauthorized third parties.

90. Knowing that thieves stole her PII, including her Social Security number and/or driver's license number and other PII that she was required to provide to Defendants, and knowing that her PII will likely be sold on the dark web, has caused Plaintiff Thomas great anxiety.

91. Plaintiff Thomas has a continuing interest in ensuring that her PII that, upon information and belief, remains in the possession of Defendants, is protected and safeguarded from future data breaches.

As a result of the Data Breach, Plaintiff Thomas is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

### **CLASS ALLEGATIONS**

92. Plaintiff brings this nationwide class action pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), individually and on behalf of all members of the Class:

All natural persons residing in the United States whose PII was compromised in the Data Breach initially discovered by Defendants on or about October 3, 2021 (the “Class”).

93. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

94. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

95. **Numerosity.** The Class is so numerous that joinder of all members is impracticable. The Class includes hundreds of thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class Members is in the possession and control of Defendants and will be ascertainable through discovery.

96. **Commonality.** There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class Members, including, without limitation:

- a. Whether Defendants unlawfully maintained, lost or disclosed Plaintiff's and Class Members' PII;
- b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendants owed a duty to Class Members to safeguard their PII;
- f. Whether Defendants breached duties to Class Members to safeguard their PII;
- g. Whether cyber criminals obtained Class Members' PII in the Data Breach;
- h. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Defendants owed a duty to provide Plaintiff and Class Members notice of this Data Breach, and whether Defendants breached that duty to provide timely notice;
- j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;
- k. Whether Defendants' conduct was negligent;
- l. Whether Defendants' conduct violated federal law;
- m. Whether Defendants' conduct violated state law; and
- n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

97. **Typicality.** Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had her personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the uniform misconduct of Defendants, described throughout this Complaint, and assert the same claims for relief.

98. **Adequacy.** Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

99. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendants' wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

100. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendants to have to choose between differing means of upgrading their data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

101. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

102. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and
- e. Whether Plaintiff and Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

**FIRST CLAIM**  
***Negligence***

103. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 102.

104. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

105. The legal duties owed by Defendants to Plaintiff and Class Members include, but are not limited to the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class Members in Defendants' possession;
- b. To protect the PII of Plaintiff and Class Members in Defendants' possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

- c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the Data Breach.

106. Defendants’ duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the “FTC Act”), which prohibits “unfair . . . practices in or affecting commerce,” including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendants of failing to use reasonable measures to protect PII.

107. Various FTC publications and data security breach orders further form the basis of Defendants’ duty. Plaintiff and Class Members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

108. Defendants breached their duties to Plaintiff and Class Members. Defendants knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

109. Defendants knew or should have known that their security practices did not adequately safeguard the PII of Plaintiff and Class Members.

110. Through Defendants’ acts and omissions described in this Complaint, including Defendants’ failure to provide adequate security and its failure to protect the PII of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendants unlawfully breached their duty to use

reasonable care to adequately protect and secure the PII of Plaintiff and Class Members during the period it was within Defendants' possession and control.

111. Defendants breached the duties they owe to Plaintiff and Class Members in several ways, including:

- a. Failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' PII and thereby creating a foreseeable risk of harm;
- b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;
- c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and
- d. Failing to timely and accurately disclose to Plaintiffs and Class Members that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

112. Due to Defendants' conduct, Plaintiff and Class Members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used for identity theft and other types of financial fraud against them immediately and for years to come.

113. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately \$219.00 to \$358.00 per year.

114. As a result of Defendants' negligence, Plaintiff and Class Members suffered injuries that may include:

- (i) actual identity theft;



- (ii) the lost or diminished value of PII;
- (iii) the compromise, publication, and/or theft of PII;
- (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;
- (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;
- (vi) the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession;
- (vii) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

115. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and Class Members suffered was the direct and proximate result of Defendants' negligent conduct.

**SECOND CLAIM**  
***Negligence Per Se***

116. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 115.

117. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The

FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

118. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members due to the valuable nature of the PII at issue in this case—including Social Security numbers.

119. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

120. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

121. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

122. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

- i. actual identity theft;
- ii. the lost or diminished value of PII;

- iii. the compromise, publication, and/or theft of PII;
- iv. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;
- v. lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;
- vi. the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession;
- vii. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

123. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and members of the Classes have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

**THIRD CLAIM**  
***Breach of Implied Contract***

124. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 123.

125. When Plaintiff and Class Members provided their PII to Defendants in exchange for Defendants' products and services, they entered into implied contracts with

Defendants under which—and by mutual assent of the parties—Defendants agreed to take reasonable steps to protect their PII.

126. Defendants solicited and invited Plaintiff and Class Members to provide their PII as part of Defendants' regular business practices and as essential to the sales and employment transactions entered into between Defendants on the one hand and Plaintiff and Class Members on the other. This conduct thus created implied contracts between Plaintiff and Class Members on the one hand, and Defendants on the other hand. Plaintiff and Class Members accepted Defendants' offers by providing their PII to Defendants in connection with their purchases from and employment with Defendants.

127. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards.

128. Defendants' implied promise to safeguard Plaintiff and Class Members' PII is evidenced by a duty to protect and safeguard PII that Defendants required Plaintiff and Class Members to provide as a condition of entering into consumer transactions and employment relationships with Defendants.

129. Plaintiff and Class Members paid money to Defendants to purchase products or services from. Plaintiff and Class Members reasonably believed and expected that Defendants would use part of the funds received as a result of the purchases or services provided to obtain adequate data security. Defendants failed to do so.

130. Plaintiff and Class Members, on the one hand, and Defendants, on the other hand, mutually intended—as inferred from customers’ continued use of Defendants’ services—that Defendants would adequately safeguard PII. Defendants failed to honor the parties’ understanding of these contracts, causing injury to Plaintiff and Class Members.

131. Plaintiff and Class Members value data security and would not have provided their PII to Defendants in the absence of Defendants’ implied promise to keep the PII reasonably secure.

132. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendants.

133. Defendants breached their implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

134. As a direct and proximate result of Defendants’ breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

**FOURTH CLAIM**  
***Unjust Enrichment***

135. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 134.

136. Defendants benefited from receiving Plaintiff’s and Class members’ PII by their ability to retain and use that information for their own benefit. Defendants understood this benefit.

137. Defendants also understood and appreciated that Plaintiff and Class Members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

138. Plaintiff and Class Members who were customers of Defendants conferred a monetary benefit upon Defendants in the form of monies paid for services from Defendants.

139. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants also benefited from the receipt of Plaintiff and Class Members' PII, as Defendants used it to facilitate the transfer of information and payments between the parties.

140. The monies that Plaintiff and Class Members paid to Defendants for products and services were to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

141. Defendants also understood and appreciated that Plaintiff and Class Members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

142. But for Defendants' willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and untrusted with Defendants. Indeed, if Defendants had informed Plaintiff and Class Members that their data and cyber security measures were inadequate, Defendants would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

143. As a result of Defendants' wrongful conduct, Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Defendants continue to benefit and profit from their retention and use of the PII while its value to Plaintiff and Class Members has been diminished.

144. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiff and Class Members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

145. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the amount Plaintiff and Class Members paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

146. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

147. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

**FIFTH CLAIM**  
***Declaratory Judgment***

148. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 147.

149. Defendants owe duties of care to Plaintiff and Class Members that require Defendants to adequately secure their PII.

150. Defendants still possess Plaintiff and Class Members' PII.

151. Defendants do not specify in the Notice of Data Breach letters what steps they have taken to prevent a data breach from occurring again.

152. Plaintiff and Class Members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

153. Plaintiff, therefore, seeks a declaration that (1) each of Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

- a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
- b. Engaging third-party security auditors and internal personnel to run automated security monitoring;



- c. Auditing, testing, and training their security personnel regarding any new or modified procedures;
- d. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;
- e. Conducting regular database scanning and security checks;
- f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- g. Purchasing credit monitoring services for Plaintiff and Class Members for a period of ten years; and
- h. Meaningfully educating Plaintiff and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, request judgment against Defendants and that the Court grant the following:

- 1. An order certifying the Class as defined herein, and appointing Plaintiff and her counsel to represent the Class;
- 2. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiff and Class Members;
- 3. An order requiring Defendants to:
  - a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on

- Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
- b. Engage third-party security auditors and internal personnel to run automated security monitoring;
  - c. Audit, test, and train their security personnel regarding any new or modified procedures;
  - d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;
  - e. Conduct regular database scanning and security checks;
  - f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
  - g. Purchase credit monitoring services for Plaintiff and Class Members for a period of ten years; and
  - h. Meaningfully educate Plaintiff and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.
4. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiff and all Class Members;
  5. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;
  6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

7. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and
8. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands this matter be tried before a jury.

Respectfully Submitted,

**CHESTNUT CAMBRONNE PA**

November 23, 2021

/s/ Bryan L. Bleichner  
Bryan L. Bleichner (MN #0326689)  
Jeffrey D. Bores (MN #227699)  
Christopher P. Renz (MN #0313415)  
100 Washington Avenue South, Suite 1700  
Minneapolis, MN 55401  
Telephone: (612) 339-7300  
Fax: (952) 336-2940  
*bbleichner@chestnutcambronne.com*  
*jbores@chestnutcambronne.com*  
*crenz@chestnutcambronne.com*

Terence R. Coates\*  
Justin C. Walker\*  
**MARKOVITS, STOCK & DEMARCO, LLC**  
3825 Edwards Road, Suite. 650  
Cincinnati, OH 45209  
Telephone: (513) 651-3700  
Fax: (513) 665-0219  
*tcoates@msdlegal.com*  
*jwalker@msdlegal.com*

*Attorneys for Plaintiff and Putative Class*

\* Pro Hac Vice Application Forthcoming